

AMENDMENTS TO THE CLAIMS

Claims 1-48 (Cancelled)

Claim 49 (New) A storage-medium rental system in which a rental agent provides, to a user, a portable storage medium storing a digital work having a right of use that is rented from the rental agent to the user, the storage-medium rental system comprising:

 a portable storage medium that stores the digital work by storing therein content information that is generated by encrypting the digital work based on a content key, and that stores rental disc identification information, as disc identification information, indicating that the portable storage medium is a disc for rental;

 a portable semiconductor memory that has an area for securely storing information;

 a rental-shop apparatus that generates right information relating to a right to use the digital work stored by the portable storage medium, and that securely writes the generated right information to the area of the portable semiconductor memory when the portable semiconductor memory is mounted to the rental-shop apparatus at a time of the user renting the portable storage medium; and

 a playback apparatus that receives an instruction from the user to play back the digital work, that securely reads the generated right information from the area of the portable semiconductor memory, that judges whether the digital work is allowed to be used, based on the read right information, and when judging that the digital work is allowed to be used, that obtains the content information from the portable storage medium and plays back the digital work based on the content information,

wherein, when the digital work stored in the portable storage medium is played back, the portable semiconductor memory and the portable storage medium are mounted in the playback apparatus,

wherein the rental-shop apparatus securely writes the generated right information including an encrypted content key into the area of the portable semiconductor memory, the encrypted content key being generated by encrypting the content key using a device key;

wherein the portable semiconductor memory includes the device key prestored in the area, the device key being unique to the portable semiconductor memory, and includes a decryption unit operable to decrypt the encrypted content key stored in the area using the device key stored in the area to generate the content key, and output the generated content key, and

wherein the playback apparatus, upon receipt of the instruction from the user to play back the digital work, reads the disc identification information from the portable storage medium, and judges whether the read disc information is rental disc identification information or sales disc identification information, and when judging that the read disc identification is rental disc identification information, receives the content key from the portable semiconductor memory and generates the digital work by decrypting the read content information using the received content key.

Claim 50 (New) The storage-medium rental system of claim 49,

wherein the portable storage medium stores first identification information identifying the digital work in correspondence with the content information,

wherein the rental-shop apparatus writes, into the area, the right information including

second identification information for identifying the digital work, and
wherein the playback apparatus compares the first identification information stored in the portable storage medium with the second identification information included in the read right information, and when the first identification information and the second identification information match, judges that the digital work obtained by decrypting the content information corresponding to the first identification information is allowed to be used.

Claim 51 (New) The storage-medium rental system of claim 49, wherein the portable semiconductor memory performs mutual authentication with the rental-shop apparatus, and allows the rental-shop apparatus to write the right information only when the mutual authentication is successful.

Claim 52 (New) The storage-medium rental system of claim 49, wherein the portable semiconductor memory performs mutual authentication with the playback apparatus, and allows the playback apparatus to read the right information only when the mutual authentication is successful.